Kali Linux - End-to-end penetration testing solutions

IN HINDI

Machhindra kalan

DIGITAL DOWNLOAD हिंदी

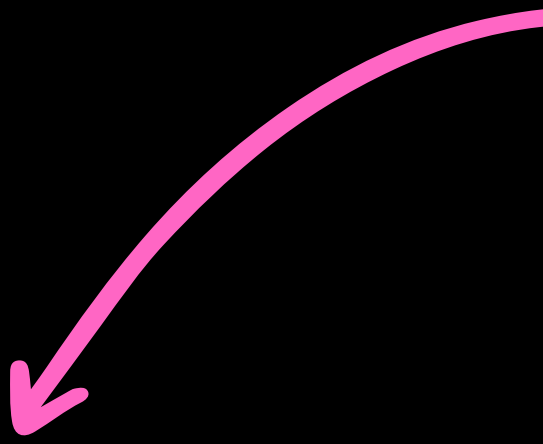
Kali Linux - End-to-end penetration testing solutions

Thanks for purchasing this Digital Download.

What's the success?

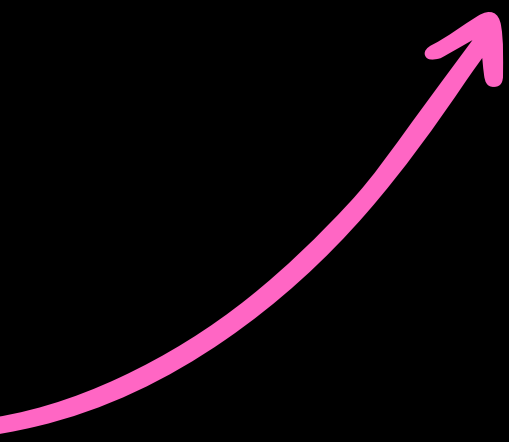
“We learn from failure, not from success!”
— Bram Stoker, Dracula

Please Keep this PDF in a safe place!



SUBSCRIBE TO FREE EBOOKS

www.cprogrammingbookinhindi.com



Kali Linux - End-to-end penetration testing solutions in Hindi

Copyright © 2017 by Machhindra Kalan

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

Trademarked names may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, we use the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Lead Editor: Machhindra Kalan

Distributed to the book trade worldwide by Web Study Lab Pvt Ltd, Location - Mumbai, Palava city Pin 421204

E-mail: machhi29@gmail.com, or

Visit: www.cprogrammingbookinhindi.com

For information on translations, please contact Web Study Lab Pvt Ltd, Location - Mumbai, Palava city Pin 421204

Phone +91 86555-67778

The information in this book is distributed on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this work, the author shall not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this book.

This book
is dedicated
to those

who really wants
to be a

KALI LINUX - END-TO-END PENETRATION TESTING SOLUTIONS

INDEX OF CONTENTS

TABLE OF CONTENT

Kali – An Introduction……..1
- Introduction
- Configuring Kali Linux
  - Getting ready
  - How to do it...
  - How it works...
  - Configuring the Xfce environment
  - How to do it...
  - Configuring the Mate environment
  - How to do it...
  - Configuring the LXDE environment
  - How to do it...
  - Configuring the e17 environment
  - How to do it...
  - Configuring the KDE environment
  - How to do it...
  - Prepping up with custom tools
  - Getting ready
  - How to do it...
  - Dnscan
  - Subbrute
  - Dirsearch Pentesting
  - VPN's ike-scan
  - Getting ready
  - How to do it...
  - Cracking the PSK
  - How it works...
  - Setting up proxychains
  - How to do it..
  - Using proxychains with tor
  - Going on a hunt with Routerhunter
  - Getting ready
  - How to do it..

Gathering Intel and Planning Attack Strategies……..... 51
- Introduction
- Getting a list of subdomains
  - Fierce
    - How to do it...
  - DNSdumpster
    - How to do it...
  - Using Shodan for fun and profit
    - Getting ready
    - How to do it...
  - Shodan Honeyscore
    - How to do it...
  - Shodan plugins
    - How to do it...
    - See also

Using Nmap to find open ports
How to do it...
Using scripts
See also
Bypassing firewalls with Nmap
TCP ACK scan
How to do it...
How it works...
TCP Window scan
How to do it...
Idle scan
How to do it...
How it works...
Searching for open directories
The dirb tool
How to do it...
There's more...
See also
Performing deep magic with Dmitry
How to do it...
Hunting for SSL flaws
How to do it...
See also
Exploring connections with intrace
How to do it...
Digging deep with theharvester
How to do it...
How it works...
Finding the technology behind web apps
How to do it...
Scanning IPs with masscan
How to do it...
Sniffing around with Kismet
How to do it...
Testing routers with firewalk
How to do it...
How it works...
Vulnerability Assessment…… 110
Introduction
Using the infamous Burp
How to do it...
Exploiting WSDLs with Wsdler
How to do it...
Using Intruder
How to do it...
Web app pentest with Vega
Getting ready
How to do it...
Exploring SearchSploit
How to do it...
Exploiting routers with RouterSploit

Getting ready
How to do it...
Using the scanners command
Using creds
Using Metasploit
How to do it...
Automating Metasploit
How to do it...
Writing a custom resource script
How to do it...
Databases in Metasploit
How to do it...
Web App Exploitation – Beyond OWASP Top 10…….. 163
Introduction
Exploiting XSS with XSS Validator
Getting ready
How to do it...
Injection attacks with sqlmap
How to do it...
See also
Owning all .svn and .git repositories
How to do it...
Winning race conditions
How to do it...
See also
Exploiting JBoss with JexBoss
How to do it...
Exploiting PHP Object Injection
How to do it...
See also
Backdoors using web shells
How to do it...
Backdoors using meterpreters
How to do it...
Network Exploitation on Current Exploitation…….. 205
Introduction
Man in the middle with hamster and ferret
Getting ready
How to do it...
Exploring the msfconsole
How to do it...
Railgun in Metasploit
How to do it...
There's more...
Using the paranoid meterpreter
How to do it...
There's more...
A tale of a bleeding heart
How to do it...
Redis exploitation
How to do it...

Say no to SQL – owning MongoDBs
Getting ready
How to do it...
Embedded device hacking
How to do it...
Elasticsearch exploit
How to do it...
See also
Good old Wireshark
Getting ready
How to do it...
There's more...
This is Sparta!
Getting ready
How to do it...
Wireless Attacks – Getting Past Aircrack-ng…… 259
Introduction
The good old Aircrack
Getting ready
How to do it...
How it works...
Hands on with Gerix
Getting ready
How to do it...
Dealing with WPAs
How to do it...
Owning employee accounts with Ghost Phisher
How to do it...
Pixie dust attack
Getting ready
How to do it...
There's more...
Password Attacks – The Fault in Their Stars……292
Introduction
Identifying different types of hash in the wild!
How to do it...
MD5
MySQL less than v4.1
MD5 (WordPress)
MySQL 5
Base64 encoding
There's more...
Using hash-identifier
How to do it...
Cracking with patator
How to do it...
Cracking hashes online
How to do it...
Hashkiller
Crackstation
Online HashCrack

Playing with John the ripper
How to do it...
There's more...
Johnny Bravo!
How to do it...
Using cewl
How to do it...
Generating word list with crunch
How to do it...
Have Shell Now What?..... 329
Introduction
Spawning a TTY Shell
How to do it...
There's more...
Looking for weakness
How to do it...
Horizontal escalation
How to do it...
Vertical escalation
How to do it...
Node hopping – pivoting
How to do it...
There's more…
Privilege escalation onNWindows
How to do it...
Using PowerSploit
How to do it…
There's more…
Pulling plaintext passwords with mimikatz
How to do it…
Dumping other saved passwords from the machine
How to do it...
Pivoting into the network
How to do it...
Backdooring for persistence
How to do it...
Buffer Overflows…… 381
Introduction
Exploiting stack-based buffer overflows
How to do it...
Exploiting buffer overflow on real software
Getting ready
How to do it...
SEH bypass
How to do it...
See also
Exploiting egg hunters
Getting ready
How to do it...
See also
An overview of ASLR and NX bypass

How to do it...
See also
Playing with Software-Defined Radios…….. 432
Introduction
Radio frequency scanners
Getting ready
How to do it...
Hands-on with RTLSDR scanner
How to do it...
Playing around with gqrx
How to do it...
There's more...
Kalibrating device for GSM tapping
How to do it...
There's more...
Decoding ADS-B messages with Dump1090
How to do it...
There's more...
Kali in Your Pocket – NetHunters and Raspberries……..... 457
Introduction
Installing Kali on Raspberry Pi
Getting ready
How to do it...
Installing NetHunter
Getting ready
How to do it...
Superman typing – HID attacks
How to do it...
Can I charge my phone?
How to do it...
Setting up an evil access point
How to do it...
Writing Reports…….. 484
Introduction
Generating reports using Dradis
How to do it...
Using MagicTree
How to do it...
There's more...

INTRODUCTION

काली को पहली बार 2012 में पूरी तरह से नई वास्तुकला के साथ पेश किया गया था। इस डेबियन आधारित डिस्ट्रो को 300 से अधिक उपकरणों के साथ जारी किया गया था जो पैठ परीक्षण और डिजिटल फोरेंसिक के लिए विशेष थे। इसका रखरखाव और वित्त पोषण सिक्योरिटी लिमिटेड द्वारा किया जाता है, जिसमें कोर डेवलपर्स मति अहरोनी, डेवोन र्किन्स और राफेल हर्टजोग शामिल हैं।

काली 2.0 2016 में नए अपडेट और नए डेस्कटॉप वातावरण जैसे KDE, Mate, LXDE, e17 और Xfce बिल्ड के साथ तस्वीर में आया।

जबकि काली पहले से ही दुनिया भर में पैठ परीक्षकों की मदद करने के लिए सैकड़ों अद्भुत उपकरणों और उपयोगिताओं के साथ पहले से सुसज्जित हैं, इस अध्याय में कुशलतापूर्वक काम करने के लिए, हम मुख्य रूप से कुछ कस्टम ट्विक्स को कवर करेंगे जिनका उपयोग करने के लिए और भी बेहतर अनुभव करने का अनुभव उपयोगकर्ता हो सकता है।

Configuring Kali Linux

हम विभिन्न सुरक्षा वातावरण जैसे Mate, e17, Xfce, LXDE और KDE डेस्कटॉप को स्थापित और कॉनफ़िगर करने के लिए आक्रामक सुरक्षा द्वारा प्रदान किए गए आधिकारिक काली लिनक्स आईएसओ का उपयोग करेंगे।

Getting ready

इस रेसिपी के साथ शुरू करने के लिए हम आक्रामक सुरक्षा वेबसाइट पर सूचीबद्ध 64–बिट काली लिनक्स आईएसओ का उपयोग करेंगे:

https://www.kali.org/downloads/

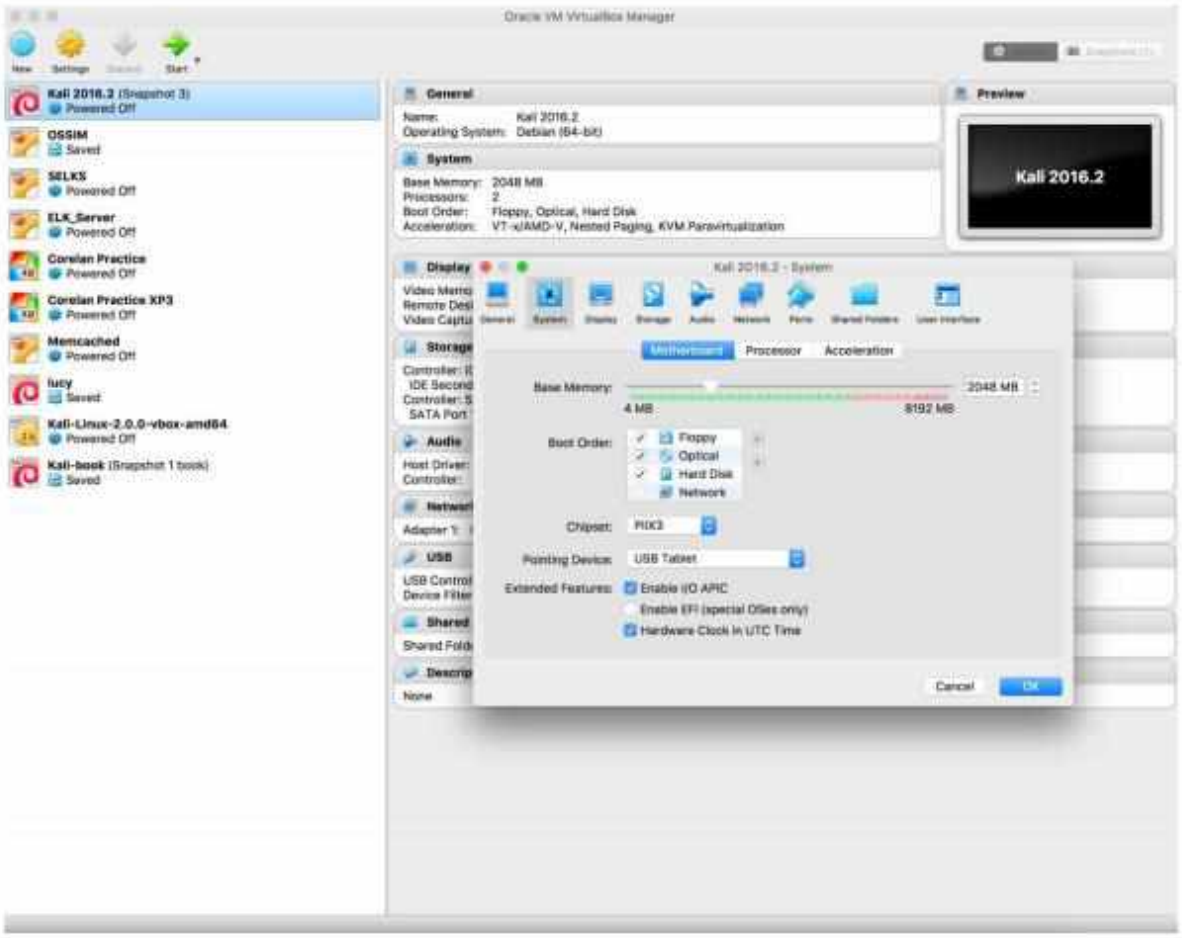
> *For users looking to configure Kali in a virtual machine such as VMware, VirtualBox, and so on, a pre-built image of the Linux can be downloaded from https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/.*

हम इस अध्याय में virtual image का उपयोग करेंगे और इसे कुछ अतिरिक्त उपकरणों के साथ अनुकूलित करेंगे।

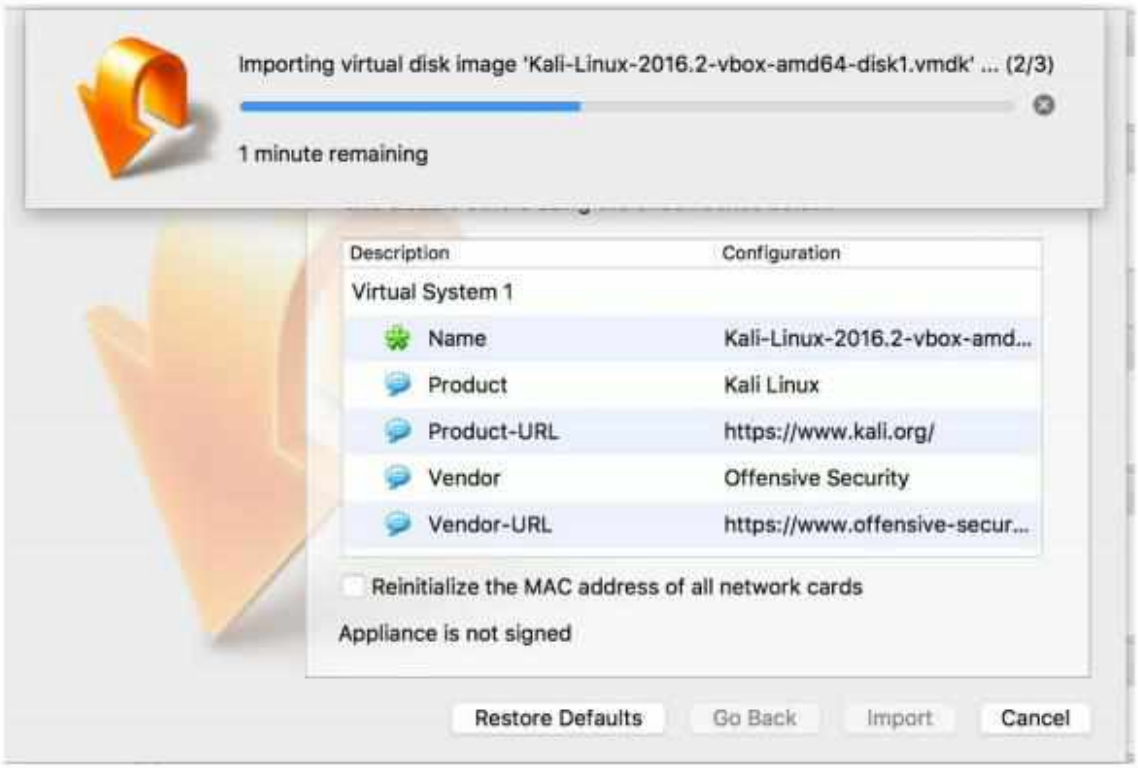
How to do it...

You can configure Kali with the help of the given steps:

1. Double-click on the VirtualBox image, it should open with VirtualBox:



2. Click Import:



3. Start the machine and enter the password as `toor`:

4. Now, Kali is started and by default is configured with the GNOME desktop environment:

Applications
Places
Wed 02:18

How it works...

पूर्व–निर्मित छवि के साथ आपको स्थापना प्रक्रिया के बारे में चिंता करने की आवश्यकता नहीं है। आप इसे तैयार समाधान के रूप में मान सकते हैं। बस रन पर क्लिक करें और वर्चुअल मशीन सामान्य मशीन की तरह लिनक्स को बूट करेगी।

Configuring the Xfce environment

Xfce यूनिक्स और यूनिक्स जैसे प्लेटफार्मों के लिए एक स्वतंत्र, तेज और हल्का डेस्कटॉप वातावरण है। इसकी शुरुआत ओलिवियर फोर्डन ने की थी 1996. Xfce नाम मूल रूप से XForms आम पर्यावरण के लिए खड़ा था, लेकिन उस समय से Xfce को दो बार फिर से लिखा गया है और अब XForms टूलकिट का उपयोग नहीं करता है।

How to do it...

To configure the Xfce environment follow the given steps:

1. We start by using the following command to install Xfce along with all plugins and goodies:

```
apt-get install kali-defaults kali-root desktop-base xfce4
xfce4-places-plugin xfce4-goodies
```

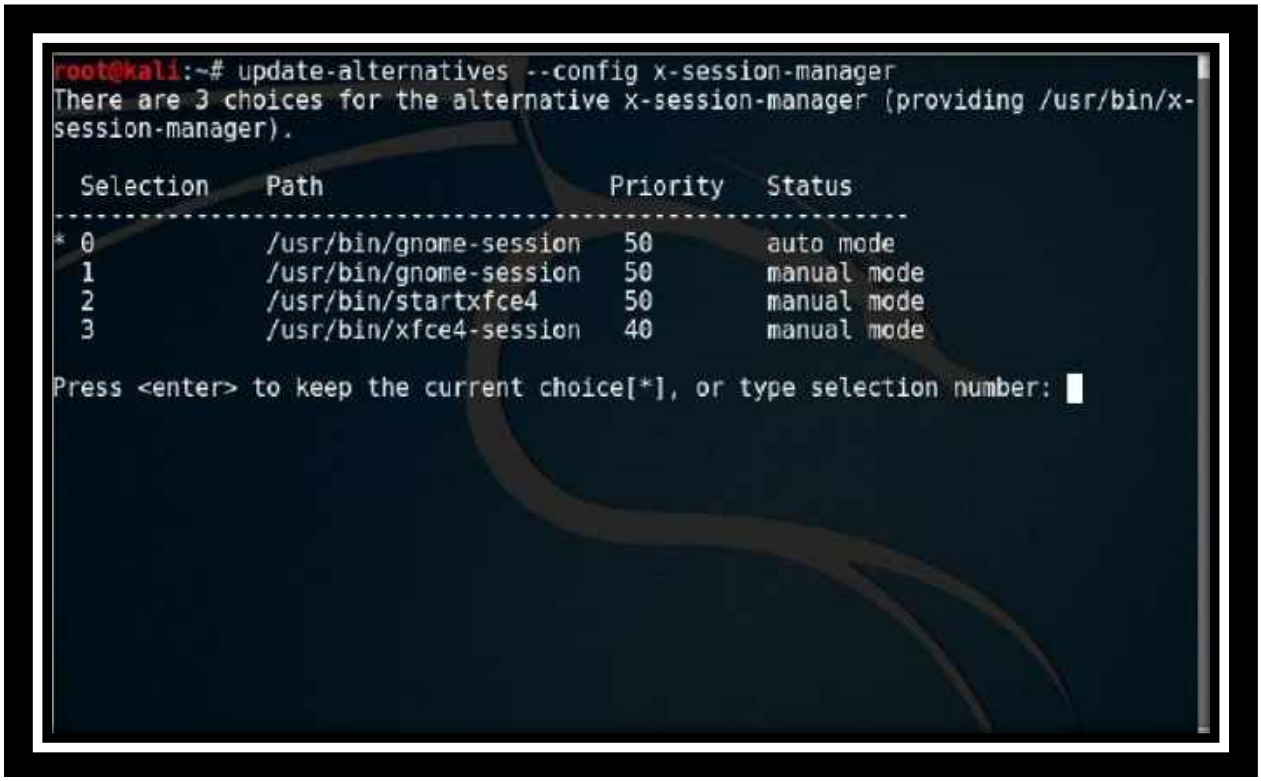
The following screenshot shows the preceding command:

2. Type v when it asks for confirmation on additional space requirements.
3. Select Ok on the dialogue box that appears.

4. We select lightdm as our default desktop manager and press the *Enter* key.
5. When the installation is complete we open a Terminal window and type the fallowing command:

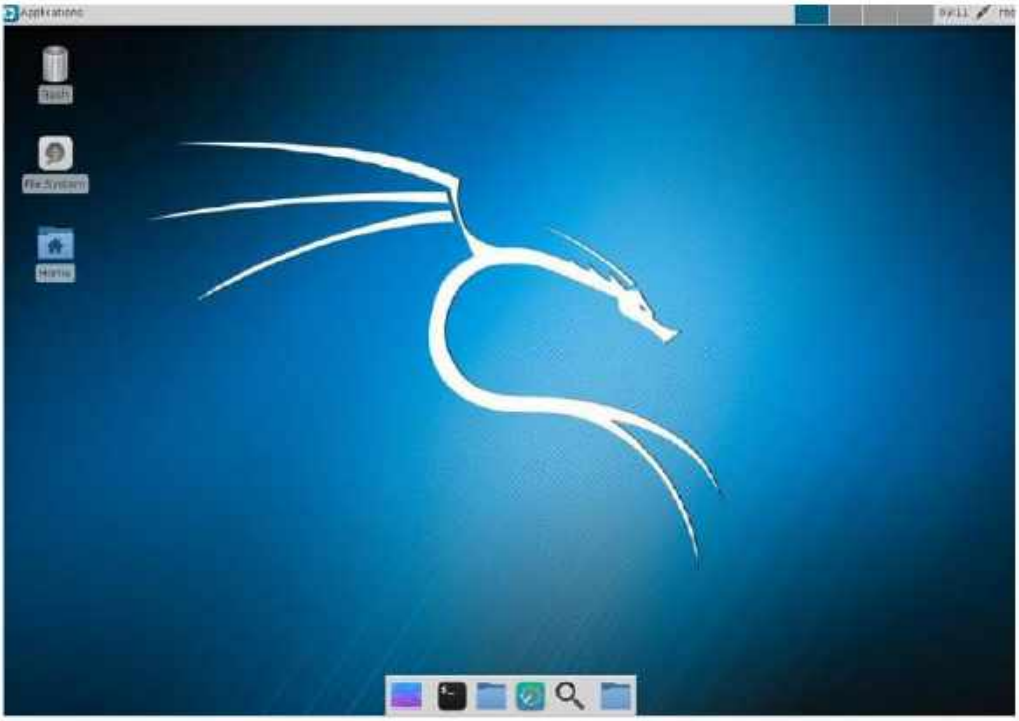
```
update-alternatives --config x-session-manager
```

The following screenshot shows the output of the preceding command:



6. Choose the option xfce4-session (in our case 3) and press the *Enter* key.

7. Log out and log in again or you can restart the machine and we will see the Xfce environment:


Applications
Trash
File System
Home

Configuring the Mate environment

मेट डेस्कटॉप वातावरण (environment) GNOME 2 की निरंतरता में बनाया गया था. यह पहली बार 2011 में जारी किया गया था.

How to do it...

To configure the Mate environment follow the given steps:

1. We start by using the following command to install the Mate environment:

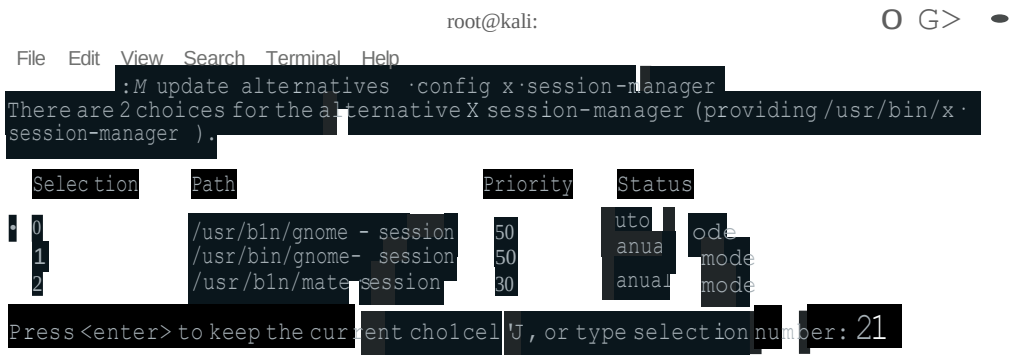
```
apt-get install desktop-base mate-desktop-environment
```

The following screenshot shows the preceding command:

2. Type v when it asks for confirmation on additional space requirements.
3. When installation is complete we will use the following command to set Mate as our default environment:

```
update-alternatives --config x-session-manager
```

4. Choose the option mate-session (in our case 2) and press the *Enter* key:



5. Log out and log in again or restart and we will see the Mate environment:

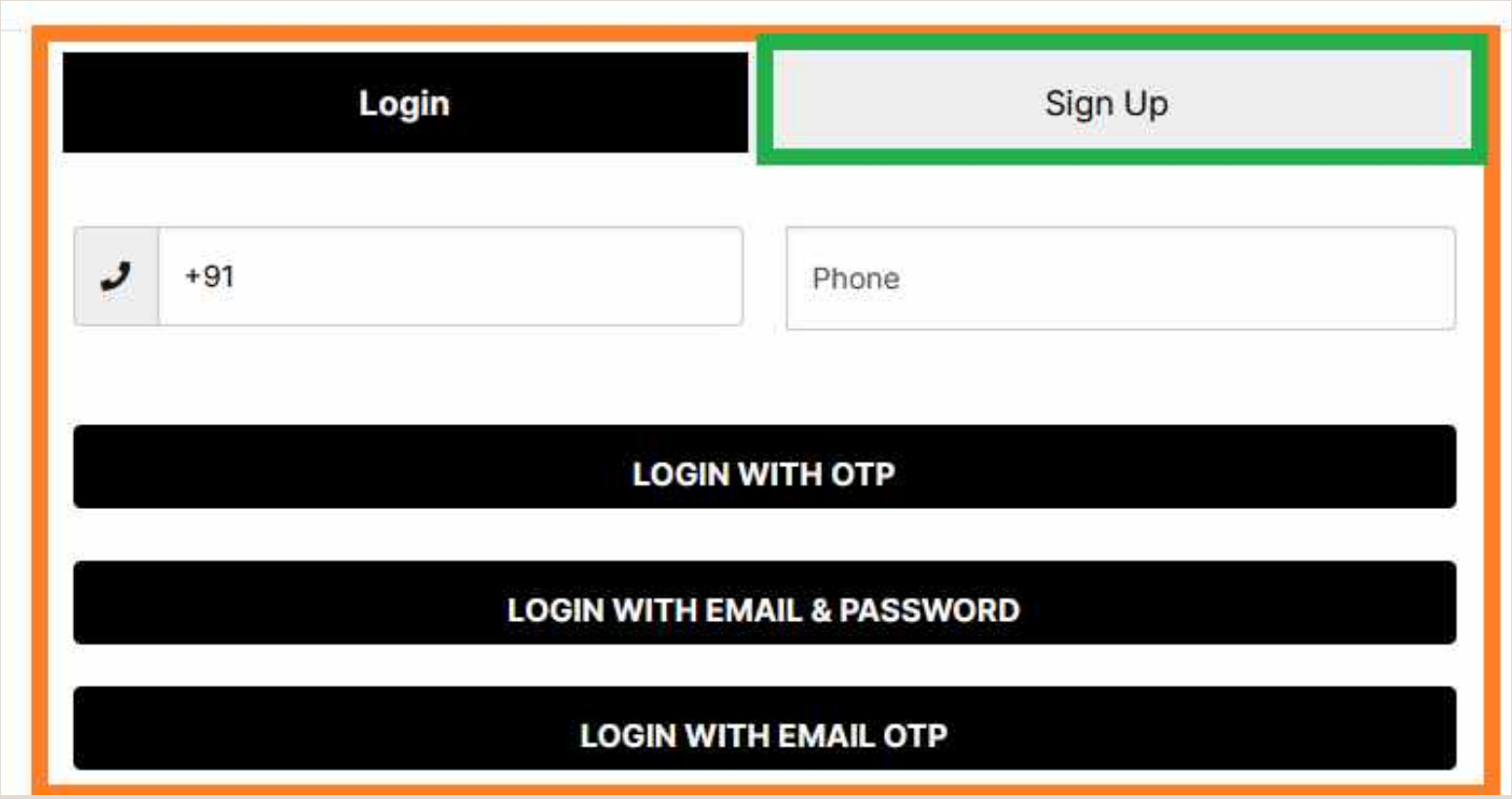
Applications
Places
System

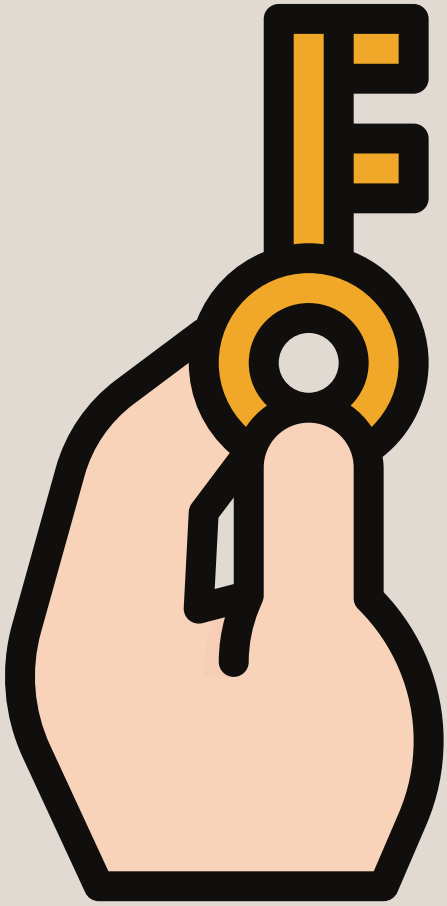
HOW TO GET COMPLETE PDF EBOOK

Pay Paytm

कोई भी **2 Ebooks** खरीदने पर **20%** डिस्काउंट- **India20**

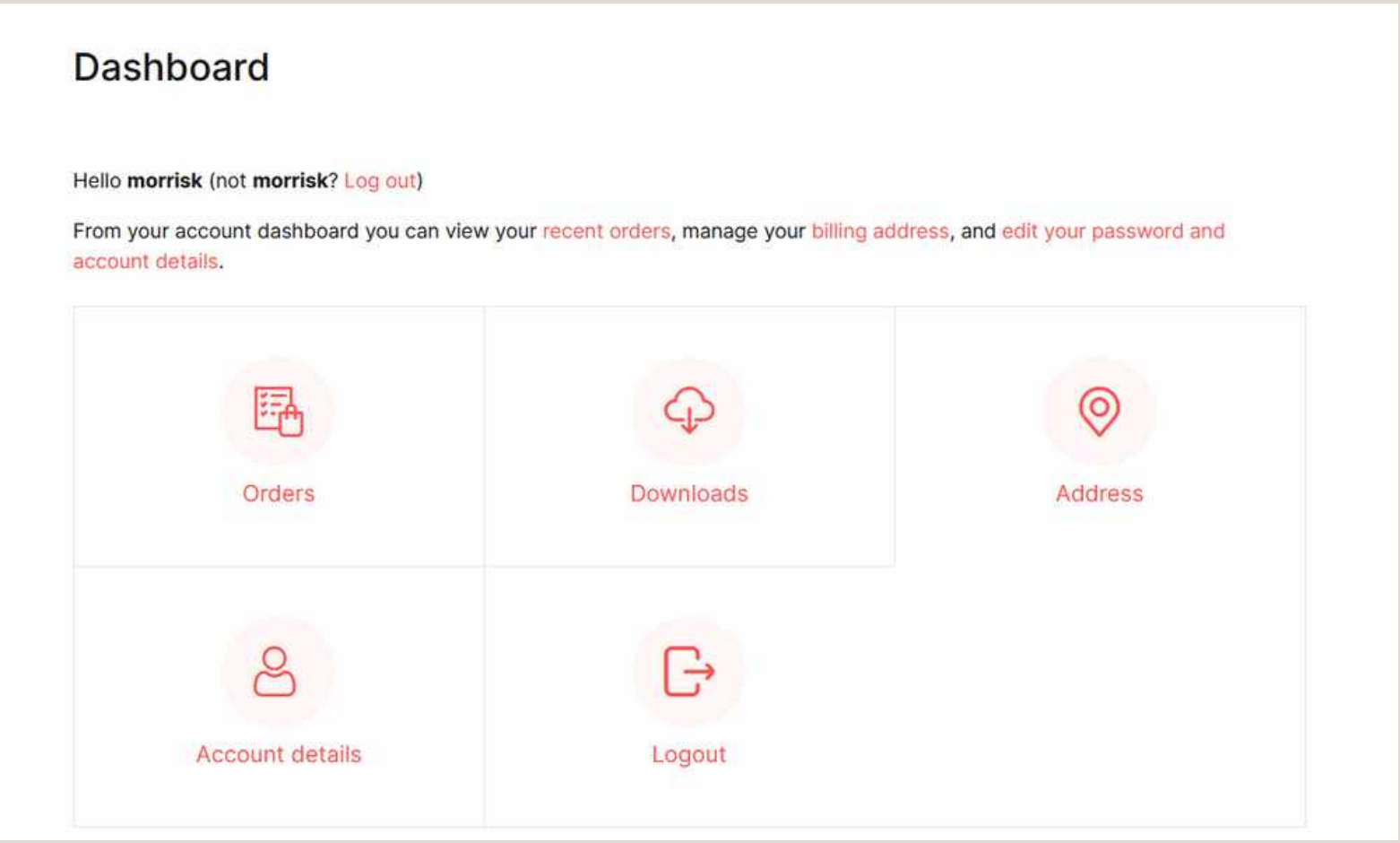
Buy Now पर क्लिक करने पर आपको **चेकआउट पेज** पर लॉगिन फॉर्म पर पहिले ईमेल से लॉगिन करना होगा।





Login Succesfull के बाद आपको पेमेंट करके Ebooks वही से डाउनलोड कर सकते है।

उसके बाद आप **My Account** पेज पर जाकर **Download** में Ebooks डाउनलोड कर सकते है।



Thank you